GeekBrains

Компьютерные сети

Сетевой уровень. Часть 3. Бесклассовая адресация

Динамическая маршрутизация. Балансировка трафика. BGP. RIP. DHCP

Введение

OSI/ISO	TCP/IP (DOD)
7. Прикладной уровень	4. Уровень приложений
6. Уровень представления	
5. Сеансовый уровень	
4. Транспортный уровень	3. Транспортный уровень
3. Сетевой уровень	2. Сетевой уровень
2. Канальный уровень	1. Уровень сетевых интерфейсов
1. Физический уровень	

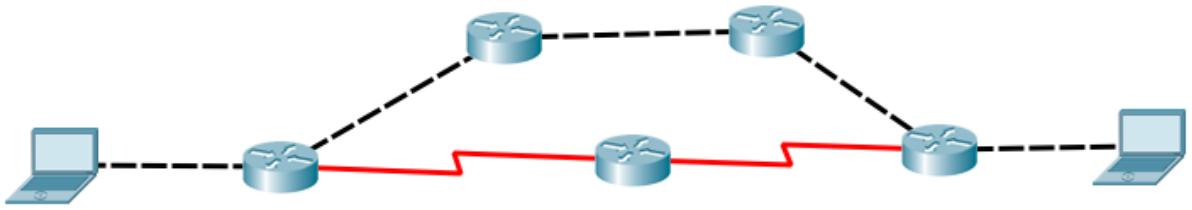
Продолжаем изучать сетевой уровень. На этом занятии мы разберем протоколы маршрутизации, а также использование протокола DHCP для назначения IP-адресов хостам.

Динамическая маршрутизация

Динамическая маршрутизация используется в средних и крупных сетях. Маршрутная информация вычисляется на основе данных, поступающих от соседних маршрутизаторов. Для обмена данными используется протокол динамической маршрутизации.

- Преимущества: быстрее настройка и проще в администрировании.
- Недостатки: требуется понимание работы протоколов, а также, в некоторых случаях, повышенная загрузка процессора маршрутизатора.

В многосвязных сетях при использовании различных протоколов маршрутизации могут задействоваться разные маршруты для передачи информации между двумя узлами. Все протоколы динамической маршрутизации делятся на 2 группы: дистанционно-векторные (Distance Vector) и протоколы состояния связи (Link State).



Дистанционно-векторные протоколы (Distance Vector) используют алгоритм кратчайшего пути для поиска маршрута до удаленной сети. Каждый переход (перенаправление) пакета с помощью маршрутизатора называют хопом (HOP). Протоколы этого типа вычисляют маршрут по количеству переходов без учета производительности канала. Примерами таких протоколов являются RIP и IGRP.

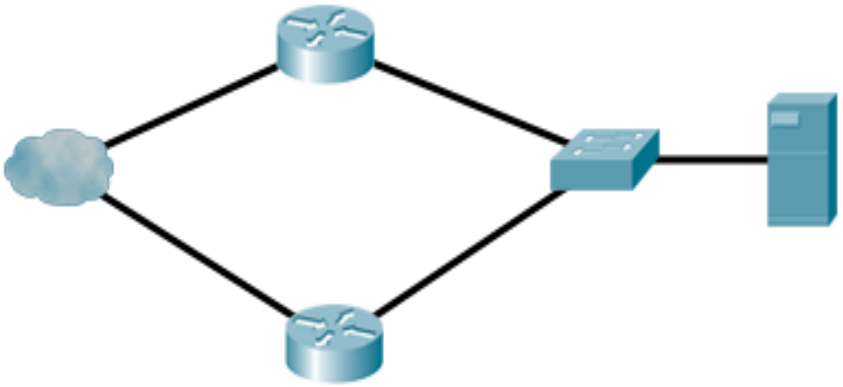
- К их преимуществам можно отнести то, что они меньше нагружают процессоры маршрутизаторов и сеть, а их главный недостаток — неэффективный учет пропускной способности и загруженности каналов. Дистанционно-векторные протоколы лучше подходят для топологий типа Hub-and-Spoke (когда, например, несколько удаленных офисов подключены к центральному офису, и весь трафик между узлами проходит через центральный офис).

Протоколы состояния связи (Link State) также называются протоколами состояния канала. Все маршрутизаторы в сети, на которых запущен протокол, содержат и постоянно обновляют три таблицы. Первая отслеживает соседние устройства, вторая содержит топологию всей сети и третья используется для маршрутизации пакетов. Данные протоколы эффективнее учитывают текущее состояние сети, но сильнее нагружают центральный процессор маршрутизатора в случае пересчета маршрута. Устройства, использующие протокол состояния связи, обладают большей информацией о сети, чем протоколы вектора расстояния. Примерами протоколов состояния связи являются: OSPF, IS-IS.

- К их недостаткам можно отнести то, что данная группа протоколов создает бóльшую нагрузку на вычислительные ресурсы, и протоколы этой группы годятся не для всех сетевых топологий.

Балансировка трафика

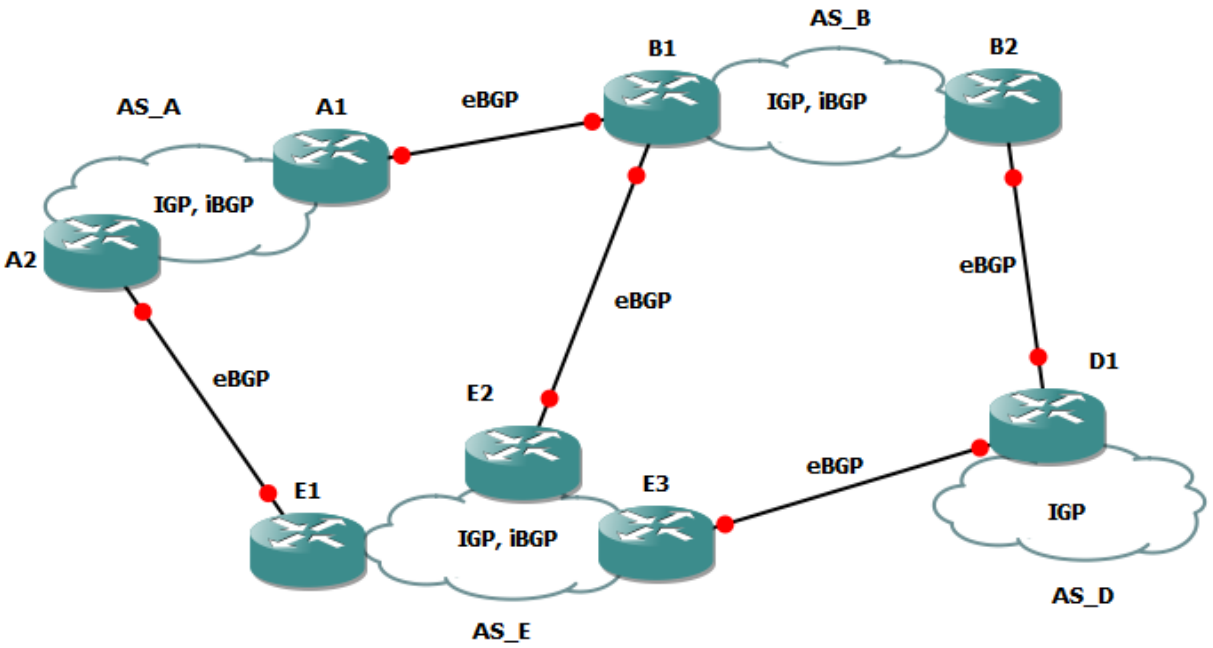
Балансировка (выравнивание) нагрузки (англ. load balancing) — это метод распределения заданий между несколькими сетевыми устройствами (например, серверами) с целью оптимизации использования ресурсов, сокращения времени обслуживания запросов, горизонтального масштабирования кластера (динамическое добавление/удаление устройств), а также обеспечения отказоустойчивости (резервирования).



BGP

Border Gateway Protocol — это основной протокол динамической маршрутизации, который используется в Интернете. Маршрутизаторы, использующие протокол BGP, обмениваются информацией о доступности сетей.

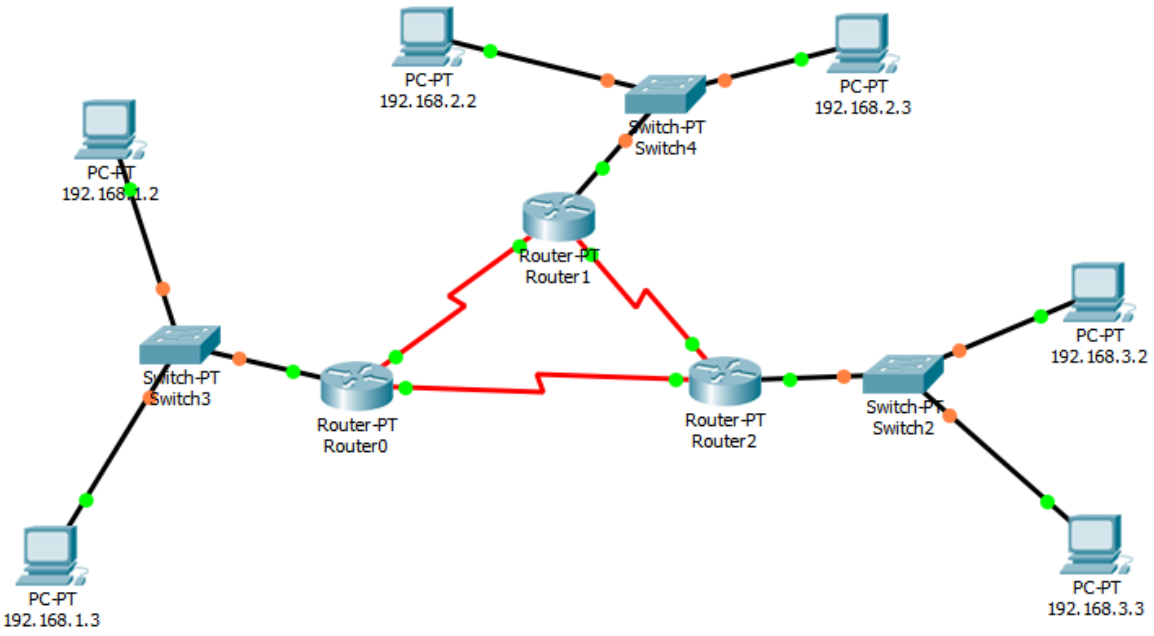
Протокол BGP нельзя отнести к дистанционно-векторным, но он использует их идею. Основой для вычисления маршрута в BGP являются правила и приоритеты для трафика, настроенные администраторами. Данный протокол в основном используется провайдерами доступа в Интернет и организациями, чьи сети или серверы должны быть доступны извне.



RIP

Routing Information Protocol — один из старейших, наиболее известных и простых протоколов маршрутизации. Использует транспортный протокол UDP и 520 порт. Чтобы маршрутизатор работал с разными сетями, достаточно настроить использование RIP-протокола и указать, о каких из используемых сетей маршрутизатор будет уведомлять другие маршрутизаторы. Это можно сделать и из GUI-интерфейса Cisco Packet Tracer, но в этом случае вы не сможете указать маску сети, а значит, не сможете выполнить даже простейшие задачи — например, выделить разным машинам подсети из сети 10.0.0.0.

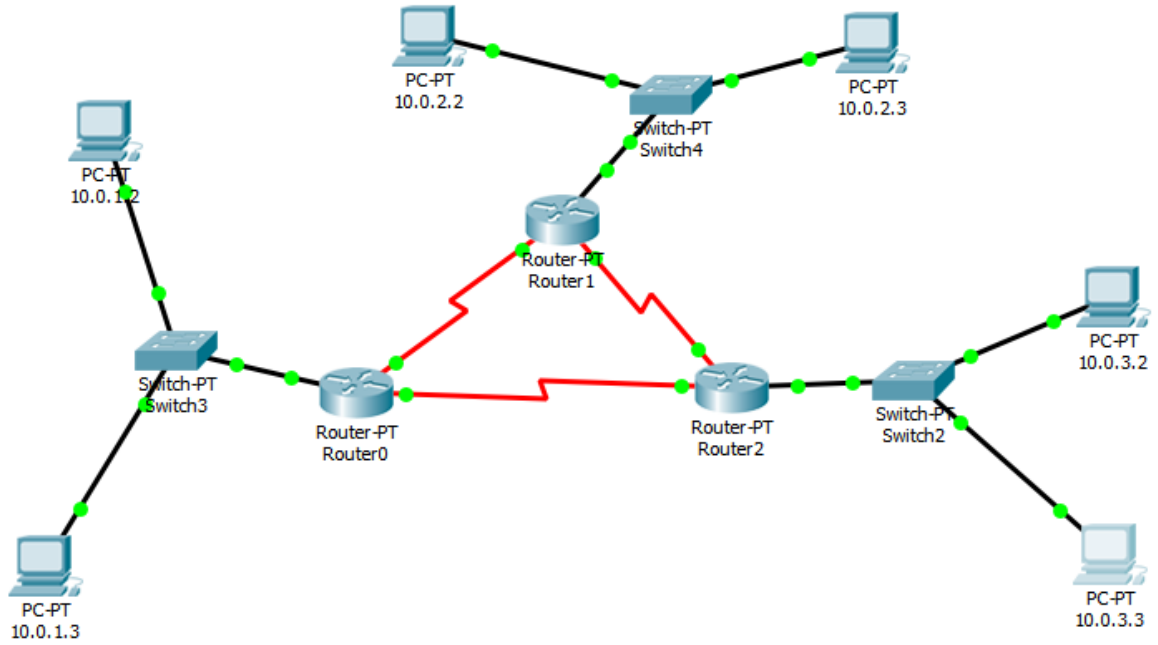
Маски в протоколе RIP не передаются, они определяются исходя из класса сети. Например, для 10.0.0.0 маска будет 255.0.0.0. Придется использовать, например, адреса вида 192.168.X.0, которые относятся к классу C.



Чтобы исправить этот недостаток, была разработана следующая версия протокола — RIP2.

RIP2

Рассмотрим следующий пример:



Он почти не отличается от приведенного выше, но IP-адреса машин назначены в сетях 10.0.1.0/24, 10.0.2.0/24,10.0.3.0/24 (бесклассовая адресация).

В такой схеме невозможно настроить маршрутизацию с помощью RIP (который поддерживает только классовую адресацию и не рассылает маски сетей), зато можно использовать RIP2.

В протоколе RIP2 появилась возможность указывать маску сети, которая также рассылается вместе с адресом сети другим маршрутизаторам.

Настроим сетевые интерфейсы:

```
Router0>ena
Router0#conf t
Router0(config)#int fa0/0
Router0(config-if)#ip addr 10.0.1.1 255.255.255.0
Router0(config-if)#no shut
Router0(config-if)#int se2/0
Router0(config-if)#ip addr 172.16.0.1 255.255.0.0
Router0(config-if)#no shut
Router0(config-if)#int se3/0
Router0(config-if)#ip addr 172.17.0.1 255.255.0.0
Router0(config-if)#no shut
Router0(config-if)#exit
```

Перейдем в настройки протокола RIP.

```
Router0(config)#route rip
```

Обязательно включим версию 2 и объявим те сети, о которых маршрутизатор будет оповещать нас, и те, через которые он это будет делать:

```
Router0(config-router)#version 2
Router0(config-router)#network 10.0.1.0
Router0(config-router)#network 172.16.0.0
Router0(config-router)#network 172.17.0.0
```

Если у данной машины имеется маршрут по умолчанию, можно рассылать и его:

```
Router0(config-router)# default-information originate
```

Осталось сделать сам маршрут по умолчанию (если, допустим, при схеме выше у Router0 имеется еще маршрут):

```
Router0(config-router)# exit
Router0(config)ip route 0.0.0.0 0.0.0.0 100.64.0.1
```

Но необходимо добавить и шлюз 100.64.0.1 и сетевой интерфейс на Router0, например на fa5/0, в сети 100.64.0.0/24.

Такие же действия, кроме двух последних пунктов, необходимо проделать и на других маршрутизаторах.

После чего можно в привилегированном режиме посмотреть маршруты:

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 2 subnets
C 10.0.1.0 is directly connected, FastEthernet0/0
R 10.0.3.0 [120/1] via 172.17.0.2, 00:00:06, Serial3/0
C 172.16.0.0/16 is directly connected, Serial2/0
C 172.17.0.0/16 is directly connected, Serial3/0
R 172.18.0.0/16 [120/1] via 172.17.0.2, 00:00:06, Serial3/0
```

DHCP

Dynamic Host Configuration Protocol, или протокол динамической конфигурации сетевых узлов — протокол, позволяющий узлам в компьютерной сети в автоматическом режиме получить IP-адрес и дополнительные параметры (маска сети, основной шлюз, доменный сервер и другие), нужные для работы в сети. Протокол построен на клиент-серверной архитектуре. В качестве сервера может выступать компьютер, маршрутизатор или коммутатор 3-го уровня.

Во время инициализации сетевого интерфейса с включенным режимом автоматической конфигурации клиент отправляет широковещательный запрос в сеть с целью обращения к DHCP-серверу. Сервер присылает ответ, сообщая информацию о необходимых сетевых параметрах. Клиент отвечает серверу, подтверждая, что он готов принять сетевые параметры и нужно зарегистрировать IP-адрес из пула за ним. Сервер подтверждает регистрацию адреса, и клиент начинает использовать назначенный ему адрес. Администратор конфигурирует диапазон адресов (сетевой пул), которые будут назначены клиентам.

Данный протокол ускоряет конфигурирование сетевых устройств и позволяет привязать IP-адреса по MAC-адресам к каждому устройству. Протокол DHCP всегда используется в беспроводных сетях.

DHCP разработан на основе протокола BOOTP, который использовался для загрузки бездисковых терминалов и назначения им сетевых адресов. DHCP обратно совместим с BOOTP, но, в отличие от него, позволяет использовать динамические конфигурации.

Порт/ID: 67, 68/UDP.

Настройка DHCP-сервера на маршрутизаторе Cisco

Настроим на Router0 DHCP-сервер.

Посмотрим доступные сервисы (увидим, что DHCP активен), а также список команд для DHCP:

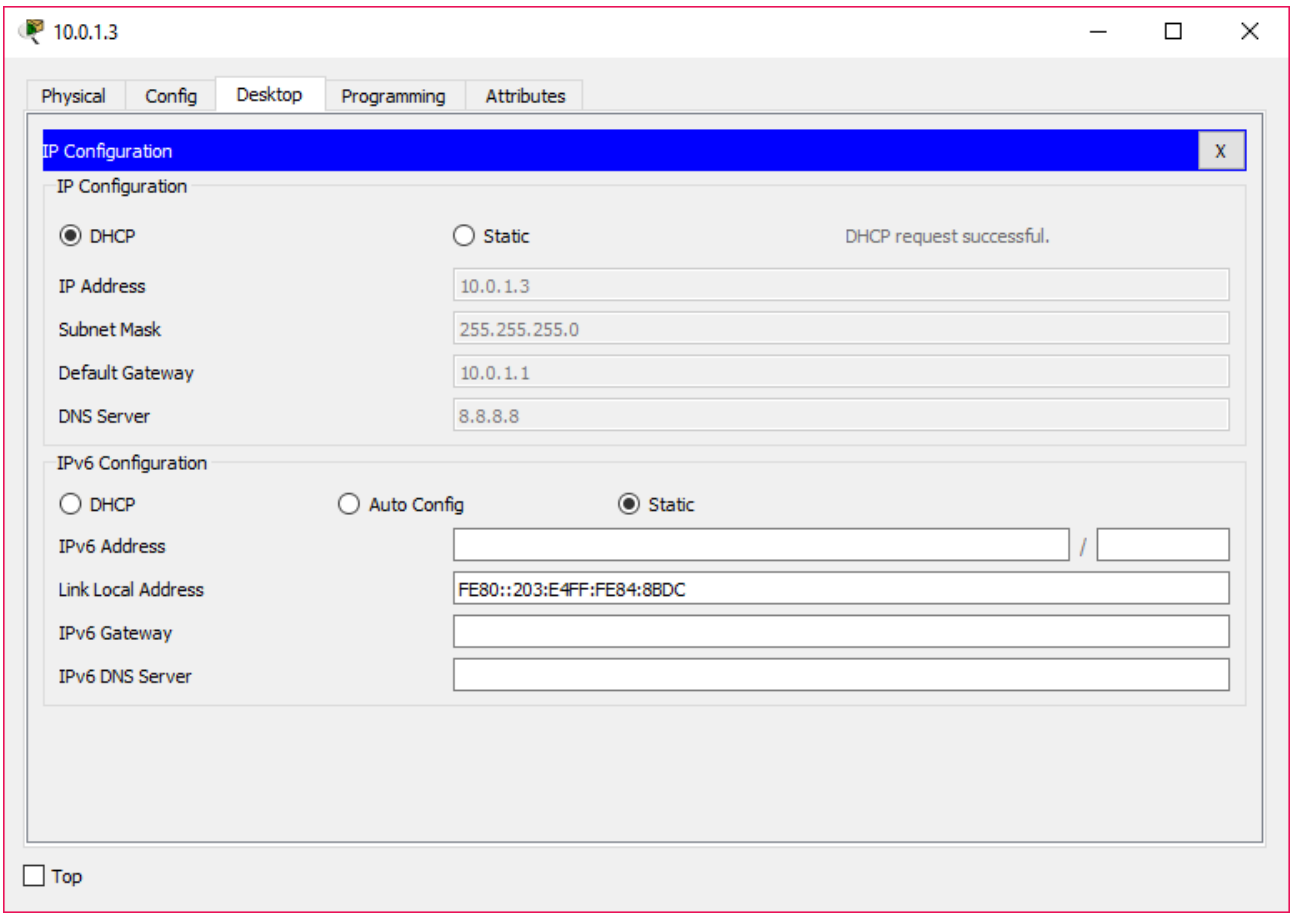
```
Router(config)#service ?
dhcp Enable DHCP server and relay agent
nagle Enable Nagle's congestion control algorithm
password-encryption Encrypt system passwords
timestamps Timestamp debug/log messages
Router(config)#ip dhcp ?
excluded-address Prevent DHCP from assigning certain addresses
pool Configure DHCP address pools
relay DHCP relay agent parameters
```

Зададим пул адресов. Сначала дадим ему название, например, pool.10.0.1, а затем добавим диапазон адресов:

```
Router(config)#ip dhcp pool pool.10.0.1
```

```
Router(dhcp-config)#?
default-router Default routers
dns-server Set name server
exit Exit from DHCP pool configuration mode
network Network number and mask
no Negate a command or set its defaults
option Raw DHCP options
Router(dhcp-config)#network 10.0.1.0 255.255.255.0
Router(dhcp-config)#default-router 10.0.1.1
Router(dhcp-config)#dns-server 8.8.8.8
```

Теперь мы можем зайти на машину 10.0.1.3 и выбрать получение DHCP-адресов автоматически.



В консоли роутера мы увидим, что были попытки назначить IP-адреса, уже занятые другими машинами статически.

```
Router(dhcp-config)#%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged
10.0.1.1.
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 10.0.1.2.
```

Можно исключить адреса из диапазона (например, заранее присвоенные статически).

```
exit
Router(config)#ip dhcp ?
excluded-address Prevent DHCP from assigning certain addresses
pool Configure DHCP address pools
```

```
relay DHCP relay agent parameters
Router(config)#ip dhcp excl
Router(config)#ip dhcp excluded-address ?
A.B.C.D Low IP address
Router(config)#ip dhcp excluded-address ?
A.B.C.D Low IP address
Router(config)#ip dhcp excluded-address 10.0.1.1 ?
A.B.C.D High IP address
<cr>
Router(config)#ip dhcp excluded-address 10.0.1.1 10.0.1.2
Router(config)#
```

Теперь осталось разобраться, как работает DHCP.

Механизм получения настроек с помощью DHCP

Первый этап — обнаружение DHCP. Сообщение рассылается бродкастно, в качестве IP-адреса отправителя используется 0.0.0.0, в качестве адреса получателя — 255.255.255.255. В качестве порта отправителя клиент использует UDP-порт 68, а в качестве порта получателя — UDP-67. Сервер — наоборот.

Если у клиента ранее был назначен IP-адрес, он может указать эту информацию, но все равно, так как сейчас этот адрес не присвоен, используется отправка пакета от 0.0.0.0 на 255.255.255.255. И даже если адрес сервера известен, может быть, мы перешли в другую сеть.

Обнаружение DHCP

DHCPDISCOVER

<table>
<tr><td colspan="4">UDP Src=0.0.0.0:68 Dest=255.255.255.255:67</td></tr>
<tr><td>OP
(тип сообщения)</td><td>HTYPE
(тип аппаратного адреса)</td><td>HLEN
(длина аппаратного адреса)</td><td>HOPS
(прыжки)</td></tr>
<tr><td>0x01
(запрос серверу)</td><td>0x01
(MAC-адрес)</td><td>0x06
(длина MAC-адреса)</td><td>0x00
(количество промежуточных маршрутизаторов)</td></tr>
<tr><td colspan="4">XID (ID транзакции)</td></tr>
<tr><td colspan="4">0x3903F326</td></tr>
<tr><td colspan="2">SECS</td><td colspan="2">FLAGS</td></tr>
<tr><td colspan="2">0x0000 (время в секундах с начала процесса получения адреса; 0, если не используется)</td><td colspan="2">0x0000</td></tr>
</table>

CIADDR (IP-адрес клиента)
0xC0A80164
YIADDR
0x00000000
SIADDR
0x00000000
GIADDR
0x00000000
CHADDR (аппаратный, т. е. MAC-адрес)
0x0000001d6057ed80
SNAME
(пустое поле)
FILE
(пустое поле)
OPTIONS
Опция DHCP 53: обнаружение DHCP
Опция DHCP 50: запрос адреса 192.168.1.100 (указан присвоенный ранее адрес)

Следующий этап — предложение в DHCP.

Север отвечает на порт 68 клиента, указывая в качестве IP-адреса отправителя свой IP-адрес, а в качестве получателя 255.255.255.255. Технически в RFC 2131, описывающем работу DHCP, говорится, что сервер должен ответить юникастом на предложенный адрес, но на практике это не совсем так. Дело в том, что сетевой интерфейс, которому еще не присвоен IP-адрес, не обязан принимать сообщения, адресованные юникастом. Не все устройства могут поддерживать такую работу, потому в RFC есть оговорка, что допускается бродкастная рассылка. На практике можно встретить как бродкастные, так и юникастные ответы сервера, но бродкастные встречаются чаще. Проверьте в Wireshark, каким образом отправляет сообщения ваш сервер.

Предложение DHCP

DHCPOFFER

UDP Src=192.168.1.1:67 Dest=255.255.255.255:68			
OP	**HTYPE**	**HLEN**	**HOPS**

0x02 (ответ клиенту)	0x01 (MAC-адрес)	0x06 (длина аппаратного адреса, то есть в данном случае для MAC-адреса — 6)	0x00 (0 прыжков — 0 маршрутизаторов)
XID (идентификатор сессии)			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x0000	
CIADDR			
0x00000000			
YIADDR (адрес, предложенный клиенту)			
0xC0A80164			
SIADDR (адрес сервера)			
0xC0A80101			
GIADDR			
0x00000000			
CHADDR (аппаратный адрес)			
0x0000001d6057ed80			
SNAME			
(пустое поле)			
FILE			
(пустое поле)			
OPTIONS			
Опция DHCP 53: предложение DHCP			
Опция DHCP 1: маска сети 255.255.255.0			
Опция DHCP 3: шлюз по умолчанию 192.168.1.1			
Опция DHCP 51: срок аренды IP-адреса — 1 день			
Опция DHCP 54: DHCP-сервер 192.168.1.1			

Теперь клиент может запросить у сервера предложенный адрес и другие параметры TCP/IP (но теоретически может и отказаться).

Запрос DHCP

DHCPREQUEST

UDP Src=0.0.0.0:68 Dest=255.255.255.255:67			
OP	**HTYPE**	**HLEN**	**HOPS**
0x01 (запрос серверу)	0x01 (MAC-адрес)	0x06 (6 октетов — для MAC)	0x00 (0 прыжков — 0 маршрутизаторов)
XID			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x0000	
CIADDR			
0xC0A80164			
YIADDR			
0x00000000			
SIADDR			
0x00000000			
GIADDR			
0x00000000			
CHADDR			
0x0000001d6057ed80			
SNAME			
(пустое поле)			
FILE			
(пустое поле)			
OPTIONS			
Опция DHCP 53: запрос DHCP			
Опция DHCP 50: запрос адреса 192.168.1.100			
Опция DHCP 54: DHCP-сервер 192.168.1.1			

И четвертый этап — подтверждение настроек сервером.

Подтверждение DHCP

DHCPACK

UDP Src=192.168.1.1:67 Dest=255.255.255.255:68			
OP	**HTYPE**	**HLEN**	**HOPS**
0x02 (от сервера — клиенту)	0x01 (MAC-адрес)	0x06 (6 байт — для MAC-адреса)	0x00 (количество прыжков)
XID			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x0000	
CIADDR			
0x00000000			
YIADDR			
0xC0A80164			
SIADDR			
0x00000000			
GIADDR			
0x00000000			
CHADDR			
0x0000001d6057ed80			
SNAME			
(пустое поле)			
FILE			
(пустое поле)			
OPTIONS			
Опция DHCP 53: подтверждение DHCP			
Опция DHCP 1: маска сети 255.255.255.0			
Опция DHCP 3: шлюз по умолчанию 192.168.1.1			

Опция DHCP 51: срок аренды IP-адреса — 1 день
Опция DHCP 54: DHCP-сервер 192.168.1.1

Только после этого клиент поднимает указанный адрес на сетевом интерфейсе и использует другие настройки.

Если срок аренды не истек, клиент может попытаться начать сразу с третьего шага.

DHCP позволяет получать не только IP-адрес, маску сети, адрес шлюза по умолчанию и DNS-сервер, но и другие параметры, такие как адрес NTP-сервера (для синхронизации времени по протоколу NTP — Network Time Protocol или SNTP — Simple Network Time Protocol), адрес TFTP-сервера (Trivial File Transfer Protocol) для загрузки бездисковых станций и т. д.

Практическое задание

Скачать файл **Lesson4Homework.pkt** (из 4 урока) либо воспользоваться уже исправленным файлом, который вы делали на 4 уроке. Но учтите, что статические маршруты имеют приоритет перед динамическими, поэтому, чтобы динамическая маршрутизация заработала, нужно сначала выключить статические маршруты командой **no ip route**.

Настроить динамическую маршрутизацию с помощью протокола RIP2.

Также в локальных сетях 3 офисов организации настройте выдачу адресов по протоколу DHCP.

Проверьте, что любые два компьютера из разных сетей попарно пингуются. Учтите, что компьютеру теперь может быть присвоен другой адрес, и поэтому актуальный IP-адрес рабочей станции надо смотреть в настройках TCP/IP либо с помощью команды **ipconfig**.

Приложите для каждого из роутеров настройки (можно вывод команды **show run**) и, кроме того, вывод **sh ip ro** (таблицу маршрутизации). Самостоятельно убедитесь, что в выводе **sh ip ro** вы видите динамическую маршрутизацию (D), а не статическую (S). Непосредственные соединения (C) пусть вас не смущают: это те маршруты, через которые отправляются ARP-запросы, так и должно быть.

Приложите файл .pkt и обязательно приведите ваши комментарии, команды, которые вы вводили, и состояние таблицы маршрутов (либо отдельным файлом .docx или .pdf перечень настроек). Скриншот прилагать не требуется.

Усложненное задание. Попробуйте использовать не три сети класса C, а три подсети сети класса A, используя бесклассовую адресацию. Учтите, что если маршруты в подсети будут идти через разные маршрутизаторы, может понадобится отключить суммаризацию маршрутов командой **no auto-summary**.

Дополнительные материалы

1. https://tools.ietf.org/html/rfc2131.
2. https://ru.wikipedia.org/wiki/RIP_(сетевой_протокол).
3. https://ru.wikipedia.org/wiki/DHCP.

Используемая литература

Для подготовки данного методического пособия были использованы следующие ресурсы.

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с. (Глава 5. Сетевой уровень.)
2. https://tools.ietf.org/html/rfc2131.
3. https://ru.wikipedia.org/wiki/RIP_(сетевой_протокол).
4. https://ru.wikipedia.org/wiki/DHCP.